OCSVM-Based Novelty Detector on PLC as a Cyber Attack and Fault Application in SCADA System

Andrés Sánchez Prisco, John Anderson Gómez-Múnera, Alejandro Giraldo-Quintero, John Freddy Duitama, Elena Romero, José David Ruiz-Ariza, Javier Jiménez-Cabas

Abstract

The central goal of an Intrusion Detection System (IDS) is to find possible attacks or abnormal behaviors within a network or system. Industrial Control Systems or SCADA Systems are increasingly robust and sophisticated, allowing remotely observing and manipulating variables in PLC controllers. Moreover, information exchange and monitoring have been integrated through the internet employing IoT in recent years, thereby causing the possibility of cyber-attacks that can risk the system and even a country's national

Keywords

Cyberattacks, SCADA System, Novelty detector, OCSVM